WHAT IS CLAIMED IS:

1. A network access device for providing network security, comprising:

a plurality of input ports;

a switching fabric for routing data received on said plurality of input ports to at least one output port; and

control logic adapted to authenticate a physical address of a user device coupled to one of said plurality of input ports, to authenticate user information provided by a user of said user device only if said physical address is valid, and to restrict access to said one of said plurality of input ports in accordance with a user policy associated with said user information only if said user information is valid.

2. The network access device of claim 1, wherein said physical address comprises a Media Access Control (MAC) address.

3. The network access device of claim 1, wherein said control logic is adapted to authenticate said user information in accordance with an IEEE 802.1x protocol.

4. The network access device of claim 1, wherein said user policy identifies an access control list.

5. The network access device of claim 1, wherein said user policy includes an access control list.

6. The network access device of claim 1, wherein said user policy identifies a Media Access Control (MAC) address filter.

7. The network access device of claim 1, wherein said user policy includes a Media Access Control (MAC) address filter.

8. The network access device of claim 1, wherein said control logic is adapted to send said user information to an authentication server and to receive an accept message from said authentication server if said user information is valid.

9. The network access device of claim 8, wherein said authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server.

10. The network access device of claim 8, wherein said accept message includes said user policy.

11. The network access device of claim 1, wherein said control logic is further adapted to assign said one of said plurality of input ports to a virtual local area network (VLAN) associated with said user information if said user information is valid

12. The network access device of claim 11, wherein said control logic is adapted to receive a message from an authentication server, wherein said message comprises a VLAN identifier (ID) associated with said user information, and to assign said one of said plurality of input ports to a VLAN associated with said VLAN ID.

13. A method for providing network security, comprising:

authenticating a physical address of a user device coupled to a port of a network access device;

authenticating user information provided by a user of said user device only if said physical address is valid; and

restricting access to said port in accordance with a user policy associated with said user information only if said user information is valid.

14. The method of claim 13, wherein said authenticating a physical address comprises authenticating a Media Access Control (MAC) address.

15. The method of claim 13, wherein said authenticating said user information comprises authenticating said user information in accordance with an IEEE 802.1x protocol.

16. The method of claim 13, wherein said restricting access comprises restricting access to said one of said plurality of input ports in accordance with an access control list.

17. The method of claim 13, wherein said restricting access comprises restricting access to said one of said plurality of input ports in accordance with a Media Access Control (MAC) address filter.

18. The method of claim 13, wherein said authenticating said user information comprises:

sending said user information to an authentication server; and

receiving an accept message from said authentication server if said user information is valid.

19. The method of claim 18, wherein said authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server.

20. The method of claim 18, wherein said receiving an accept message comprises receiving an accept message that includes said user policy.

21. The method of claim 13, further comprising:

assigning said port to a virtual local area network (VLAN) associated with said user information only if said user information is valid.

22. The method of claim 21, wherein said assigning said port to a VLAN comprises:

receiving a message from an authentication server, wherein said message comprises a VLAN identifier (ID) associated with said user information; and

assigning said port to a VLAN associated with said VLAN ID.

23. A network system, comprising:

a data communications network;

a network access device coupled to said data communications network; and

a user device coupled to a port of said network access device;

wherein said network access device is adapted to authenticate a physical address of said user device, to authenticate user information provided by a user of said user device only if said physical address is valid, and to restrict access to said port in accordance with a user policy associated with said user information only if said user information is valid.

24. The system of claim 23, wherein said physical address comprises a Media Access Control (MAC) address.

25. The system of claim 23, wherein said network access device is adapted to authenticate said user information in accordance with an IEEE 802.1x protocol.

26. The system of claim 23, wherein said user policy identifies an access control list.

27. The system of claim 23, wherein said user policy includes an access control list.

28. The system of claim 23, wherein said user policy identifies a Media Access Control (MAC) address filter.

29. The system of claim 23, wherein said user policy includes a Media Access Control (MAC) address filter.

30. The system of claim 23, further comprising:

an authentication server coupled to said data communications network;

wherein said network access device is adapted to send said user information to said authentication server and to receive an accept message from said authentication server if said user information is valid.

31. The system of claim 30, wherein said authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server.

32. The system of claim 30, wherein said accept message includes said user policy.

33. The system of claim 23, wherein said network access device is further adapted to assign said port to a virtual local area network (VLAN) associated with said user information if said user information is valid.

34. The system of claim 33, further comprising:

an authentication server coupled to said data communications network;

wherein said network access device is adapted to receive a message from said authentication server, wherein said message comprises a VLAN identifier (ID) associated with said user information, and to assign said port to a VLAN associated with said VLAN ID if said user information is valid.